5

METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT FOR DIGITAL VERIFICATION OF COLLECTED PRIVACY POLICIES IN ELECTRONIC TRANSACTIONS

Background of the Invention

10   **Field of the Invention**

The present invention relates to the use of privacy policies in computer-based

on-line commerce in which sellers and buyers of goods or services are linked via an

electronic marketplace where deals are negotiated and consummated.

15   **Description of the Related Art**

As networks of linked computers become an increasingly more prevalent concept

in everyday life, on-line interactions between buyers and sellers have become

commonplace. Transactions between a business and an individual consumer are referred

to as business-to-consumer (B2C) transactions and transactions between businesses (e.g.,

20   the sale of goods from a manufacturer to a wholesaler who uses the purchased goods to

eventually sell a product on the retail level) are referred to as business-to-business (B2B)

transactions.

As a result of this increased use of networked computers to transact business, the

concept of the electronic marketplace, referred to herein as the "E-marketplace," has

emerged and become a standard form of conducting these business transactions. For a

variety of reasons, the intermediary function provided by the E-marketplace is now an

5   everyday part of transactional commerce.

On the consumer end, E-commerce sites such as E-Bay, half.com, Ubid.com, and

AuctionPort.com provide an E-marketplace serving as a central location for negotiation

of sales and/or auctions of products or services from a seller to a consumer (e.g., bidders).

Likewise, B2B sellers provide a similar intermediary service for business transactions

10 between businesses.

A significant trade off for enjoying the convenience of e-commerce is the need to

submit to a semi-public forum what would typically be considered private information.

For example, to do business on an e-commerce site, it is usually necessary to provide any

or all of the following: name, address, telephone number, email address, credit card

15 numbers, demographic information and the like. For B2B, this information might include

banking information, pricing information, inventory information, and personal

information pertaining to company contacts. This quite naturally concerns users of

e-commerce since once submitted to the e-commerce site, the user loses control of the use

of the information by others. This invariably stops some users from utilizing e-commerce sites to make purchases, despite the convenience that they offer.

As a result of the above problems, steps have been taken to develop methods for protecting the privacy of e-commerce users while allowing the e-commerce sites to

5   function. As an example, the Platform for Privacy Preferences Project (P3P) was developed by the World Wide Web Consortium and has emerged as an industry standard providing a simple, automated way for users to gain more control over the use of personal information on websites that they visit. P3P is a standardized set of multiple-choice questions, covering all the major aspects of a website's privacy policies. Taken together,

10   they present a clear snapshot of how a site claims to handle personal information about its users. P3P-enabled websites make this information available in a standard, machine-readable format. P3P-enabled browsers can "read" this snapshot automatically and compare it to the consumer's own set of privacy preferences. P3P enhances a user's control by putting privacy policies where users can find them, in a form users can

15   understand, and most importantly, enables users to act on what they see.

While functioning adequately, use of P3P or other systems to specify privacy information in an E-marketplace can be quite cumbersome. A declaration of a privacy policy that characterizes an entire particular marketplace is difficult to identify and to

express. An E-marketplace administrator can require all participants to adhere to one

particular privacy policy, either overall or even on a section-by-section basis of the

marketplace (e.g., all electronics vendors adhere to one privacy policy, all service

providers adhere to another privacy policy, etc.), but requiring this adherence will limit

5   the number of willing seller participants. Similarly, the marketplace portal could invoke

a privacy statement that only applies to the portal itself, but not to the individual

participants available via the portal. This would likely limit the number of potential

buyers using the portal, since there would be no guarantee that the portal participants

would respect the buyers' privacy needs. The use of this information will depend on the

10   individual privacy policy of the parties involved in the transaction, and at each juncture

in the transaction, the consumer's set of privacy preferences will have to be compared with

those of each party to the transaction, an annoying and time-consuming process.

The P3P working group proposed a recommendation that an SSL (secure sockets

layer) be utilized to ensure the integrity of a P3P policy being transmitted from one party

15   to another. The effect of using an SSL is that the owner of the SSL certificate used to

secure the TCP/IP connection essentially vouches for the integrity of the policy. This

works acceptably for connections between two parties. However, in portal and

multi-hosting environments such as an E-marketplace, where the E-marketplace acts in

a middle-man capacity, the integrity can only be vouched for as between a participant and

the middle-man (the E-marketplace). Thus, an unscrupulous E-marketplace

administration could receive the P3P policy over the SSL, modify it, and send it along to

others. Likewise, an unscrupulous vendor could deny the terms of the policy as being

5   valid (after having presented the terms to the E-marketplace in the hope of drumming up

business), since the policy cannot be directly tied to the vendor

Summary of the Invention

In accordance with the present invention, parties involved in transacting business

10   in an E-marketplace (E-marketplace participants) each identify and submit to the

E-marketplace their P3P policy and/or other relevant characteristics related to their

privacy policy needs (those that they adhere to, referred to as "privacy policies"; those that

they require, referred to as "privacy preferences", or both). Submitted with the privacy

policy is a digital signature that can be tied to the owner of the web objects to which the

15   privacy policy pertains. Using a digital signature assures the integrity of the privacy

policy since it travels with the privacy policy and thus refers back to the original sender

of the policy rather than the middleman (the E-marketplace). Further, this method

5

removes the onus on the SSL certificate owner to vouch for the privacy policy of the web

objects hosted in a portal.

In an alternative embodiment, a P3P privacy policy and/or privacy policy

characteristics submitted to the portal can also be digitally signed by a trusted third

5   party/certification agent who vouches for the privacy policy implementation. Allowing

the certification group to sign the certified company's privacy policy eliminates the

manual step of looking up the company at the certification group's website.

Brief Description of the Drawings

10   Figure 1 illustrates a typical E-marketplace environment and prior art methods of

transmitting privacy information;

Figure 2 illustrates a method of enabling verification of the validity of privacy

information being shared in an E-marketplace, in accordance with the present invention;

and

15   Figure 3 is a flowchart illustrating an example of basic steps performed in

accordance with the present invention.

Detailed Description of the Preferred Embodiments

Figure 1 illustrates a typical E-marketplace environment in which the present invention can be practiced and also shows the potential for misuse of privacy policies, absent the present invention. An E-marketplace 100 is coupled to a plurality of sellers

5   104, 106, 108 and 110 via a network connection 102 (e.g., the Internet). Similarly, E-marketplace 100 is connected to a plurality of buyers 114, 116, 118, and 120 via a network connection 112. In a B2B marketplace, both buyers and sellers are businesses and typically, most participants act in both capacities at one time or another. Typically, the E-marketplace 100 will comprise a server configured to receive communications from

10   the network connections 102, 112, store information for viewing by parties connected to the network connections 102 and 112, and store other information pertaining to transactions which may occur in the E-marketplace. Sellers 104, 106, 108, and 110, and buyers 114, 116, 118, and 120, typically use PC workstations, PDA's, networks, wireless devices, or other network communication devices for accessing the E-marketplace via the

15   network connections 102 and 112.

In a typical electronic transaction using the environment illustrated in Figure 1, a seller, e.g., seller 104, will connect to E-marketplace 100 via the network connection 102 and register with the E-marketplace. Seller 104 may identify itself by a pseudonym and

typically will be required to also provide true name, address, e-mail address and other identity information for identification purposes.

As described above, a seller, e.g., seller 110, transmits its P3P policy (or other policy information) to the E-marketplace via network 102, as shown. The transmission

5   of a P3P policy by itself in this manner is referred to herein as a transmission of a "naked" P3P. A problem exists, however, because the E-marketplace can modify the naked P3P policy so that it differs from the policy presented by the seller 110, resulting in P3P policy 150'. The marketplace can then present the modified P3P policy 150' to a buyer, e.g., buyer 120, thereby creating the impression that the P3P policy 150', is that of seller 110.

10   Another problem is that the seller can deny the accuracy of the P3P policy, claiming that it was altered by the E-marketplace, the buyer, or a third party (e.g., a hacker).

Also as described above, an SSL certificate 152 can be sent from seller 110 to the E-marketplace 100 via the network connection102, along with the P3P policy 150. This will confirm to the E-marketplace (and to the client browser of seller 110) that the

15   E-marketplace is "talking" to the client browser of seller 110 and that the data sent by seller 110 was not tampered with in transit. However, the E-marketplace may be communicating with buyer 120 over a different SSL connection and thus present its own SSL certificate, SSL', to buyer 120 when transmitting the modified P3P policy 150'. Thus,

the prior art does not allow a participant communicating through a middle person (the E-marketplace) to confirm that a third party with which they are doing business is the originator of the P3P policy that purports to be theirs.

Figure 2 illustrates the present invention applied to the E-marketplace depicted in

5   Figure 1. In contrast to the naked P3P or P3P/SSL Certificate combination of Figure 1, in Figure 2, the P3P policy (or other policy information) is digitally signed, in this example by the submitter, Seller 110. Digitally signing documents is a well known process and the details regarding how the signing is accomplished are not relevant to the present invention. Any known method for digitally signing the P3P policy may be used.

10   The digitally signed P3P policy is transmitted to the E-marketplace over the network, just as the P3P and/or P3P/SSL certificate combination are transmitted as described above with respect to Figure 1. If the E-marketplace administrator (or a hacker or other unauthorized party) attempts to modify the P3P policy, the digital signature will be invalidated. Thus, when a subsequent buyer (or other person attempting to view the P3P

15   policy) attempts to verify that the policy was presented to the E-marketplace by Seller 110, the invalidated signature will identify that there has been a problem with the P3P policy, and thus the party will be made aware of the problem. The digital signature will be intact,

regardless of the number of SSL connections or traversed, as long as no one has modified the P3P policy.

Figure 3 is a flowchart illustrating an example of the basic steps performed in accordance with the present invention. At step 302, an E-marketplace participant digitally

5   signs its privacy policy (e.g., its P3P policy), and at step 304, the digitally signed privacy policy is submitted to the E-marketplace. As the middleman, the E-marketplace stores the digitally signed privacy policy for use at the appropriate time in subsequent transactions.

At step 306, a buyer identifies potential business partners who have made themselves available on the E-marketplace and who are offering goods or services of

10   interest to the buyer. The buyer then requests information regarding the potential business partners and/or the goods/services that they provide.

In one embodiment of the present invention, the digitally-signed privacy information is sent to the buyer at this time, so that it is available for the buyer to verify. However, in a preferred embodiment, the digitally-signed privacy information is

15   forwarded to the buyer in a separate step (step 308) after the buyer has selected a business partner to do business with, and if desired, not until after the contract of sale has been agreed to between the parties (pending verification of the privacy information).

At step 310, the buyer validates the integrity and ownership of the privacy policy

using known techniques by using the digital privacy key associated with the business

partner, and this allows the buyer to verify that the privacy policy has not been tampered

with since being submitted by the business partner. If the buyer has not already agreed

5   to partner with the business partner, at this point the buyer makes such an agreement, and

at step 312 the transaction is completed in the same manner as any other E-marketplace

transaction.

The method of the present invention can be performed in different sequences. In

one embodiment, the marketplace verifies signed policies during the registration process

10   and vouches for their accuracy. The marketplace can verify that the participant submitting

the P3P policy has submitted a policy that has not been tampered with, by verifying the

signature. This method requires that the participants trust the E-marketplace's vouching

procedure.

In an alternative preferred embodiment, the buyer verifies the policy of the market

15   participants at the time of the transaction. Thus, for example, when buyer 120 purchases

product or services from seller 110, the marketplace simply forwards the privacy policy

of seller 110, and the buyer verifies the seller's signature, thus verifying that the P3P

policy is the same policy sent from seller 110 to the E-marketplace during the registration

11

process. In addition, the buyer 120 can also verify the signatures of any third parties

involved in the transaction, such as, insurance carriers, shippers and the like. Further, if

there is a third party verification service that will agree to vouch for the seller, then a

digitally signed statement from that third party vouching for the seller can also be

5   confirmed as having been transmitted from the third party without tampering.

The above-described steps can be implemented using standard well-known

programming techniques. The novelty of the above-described embodiment lies not in the

specific programming techniques but in the use of the steps described to achieve the

described results. Software programming code which embodies the present invention is

10   typically stored in permanent storage of some type, such as in the permanent storage of

a workstation or server maintained by the E-Marketplace. In a client/server environment,

such software programming code may be stored with storage associated with a server.

The software programming code may be embodied on any of a variety of known media

for use with a data processing system, such as a diskette, or hard drive, or CD-ROM.

15   The code may be distributed on such media, or may be distributed to users from the

memory or storage of one computer system over a network of some type to other computer

systems for use by users of such other systems. The techniques and methods for

embodying software program code on physical media and/or distributing software code

via networks are well known and will not be further discussed herein.

Although the present invention has been described with respect to a specific

preferred embodiment thereof, various changes and modifications may be suggested to

5   one skilled in the art and it is intended that the present invention encompass such changes

and modifications as fall within the scope of the appended claims.